Security Information

20230202v2

Umetrics® Studio Security Policy

Sartorius Stedim Data Analytics AB, Östra Strandgatan 24, 903 33 Umeå, Sweden

Abstract

Sartorius Stedim Data Analytics AB is committed to ensuring the security and safety of Umetrics® Studio customer entrusted data.

Information Security and Tenant Isolation

The information security and tenant isolation policy is used to protect the security of the data you entrust with Umetrics® Studio. This policy is intended to make your data inaccessible to your competitors and anyone else outside your organization. Security is a top concern in every layer of abstraction when we build and operate this service, following the principle of Defence in Depth.

In the data security context, we refer to individual customer organizations in Umetrics® Studio as *tenants*. A tenant is a company and its subsidiaries, or any other organizational grouping that makes sense in the sales- or contractual perspective.

Data encryption

Umetrics® Studio uses Transport Layer Security (TLS) on external interfaces to the platform to protect secrecy and accuracy of transmitted data. Certificates and server configuration are regularly reviewed by third-party reviewers to verify that we always have solid configuration.

We use storage encryption to protect the data from physical theft. Encryption keys are handled using best practices according to the cloud provider.

Access control

Umetrics® Studio is composed by loosely coupled autonomous components that enforces their own data models and trust towards other services. Open Policy Agent (OPA) is used to provide a cohesive access management model that is replicated to services throughout the system.

This allows us to define access policies and enforce record ownership, and to propagate real-time access-control lists to components.

Execute isolation

User-defined functions are executed in isolation, with multiple layers of defense, from workloads of other tenants. This provides both fairness and security:

- Heavy workloads from one tenant do not impact performance of others.
- Our policy that aims to prevent advanced espionage and hackers from accessing your data.

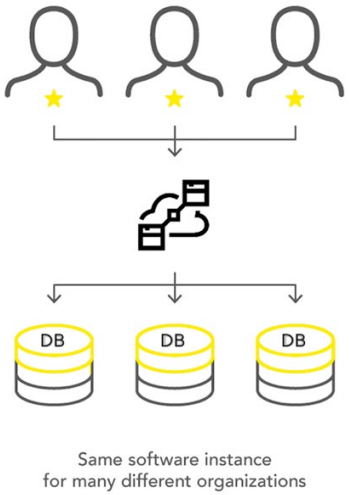
This policy is enabled through a set of measures, ranging from tenant-aware job scheduling to network segmentation and advanced OS-level protection.

Data isolation

Data records produced by end-users in Umetrics® Studio are tagged with a Tenant ID that corresponds to the end-user's organization. Records are then persisted using an isolation method that provides physical or logical separation between tenants. Where applicable:

1. *Separate data sources*: Each tenant gets their own database or storage unit.
2. *Encrypted payload*: Sensitive information in a record is encrypted using a tenant-unique cryptographic key.
3. *Row-level security*: Enforced by the persistence engine, records are not visible to end-users outside your organization. Unauthorized access attempts are denied and logged as security incidents.

The security architecture is designed to prevent data leakage between tenants and includes protection against known threats such as industry espionage.



Same software instance
for many different organizations

.

Sales and Service Contacts

For further contacts, visit Sartorius.com

Sweden

Sartorius Stedim Data Analytics AB
Östra Strandatan 24
903 33 Umeå
Phone +46 90-18 48 00